REMARKS

This communication is a full and timely response to the non-final Office Action dated September 17, 2009. Claims 1-11 and 13-16 remain pending, where claim 12 was previously canceled. By this communication, claim 16 is amended.

On page 2 of the Office Action, claim 16 is rejected under 35 U.S.C. §112, second paragraph for alleged indefiniteness. Applicant respectfully traverses this rejection. However, in an effort to expedite prosecution claim 16 is amended to address the stated concerns. Withdrawal of this rejection, therefore, is respectfully requested.

On page 3 of the Office Action, claims 1-11 and 13-16 stand rejected under 35 U.S.C. §103(a) for alleged unpatentability over *Aura* (US 6373949) in view of *Owada et al.* (US 2002/0034306). Applicant respectfully traverses this rejection.

The Office alleges that *Aura* discloses every feature recited in the claims except for using both a symmetrical algorithm and asymmetrical algorithm. *See* Office Action (09-17-09), page 4. *Owada* is relied upon in an effort to remedy this deficiency. However, the combination of *Aura* and *Owada* fails to establish a *prima facie* case of obviousness.

As discussed in a previous response, *Aura* discloses an identity protection technique in which a mobile station inputs a public key (Kd key) and an identifier (IMSI) to an algorithm to generate an encrypted identity. *See* Aura, col. 5, lines 9-12. The public key is generated by inputting a random number and private key (Kh key) into a hash function. Id., col. 4, lines 45-49. The encrypted ID and the random number are sent to a home location register HLR). Applicant notes that the random number is not encrypted.

At the HLR, *Aura* discloses that the public key (Kd key) is computed from an algorithm using the private key (Kh key) and random number. Id., col. 5, lines 33-37. The subscriber identity is then deciphered from an algorithm using the public key (Kd key) and the encrypted ID.

The process of *Aura* can be summarized through the following equation:

1st terminal: IMSI ID + KD Key (public key) + Cipher Algorithm → encrypted ID (1)

Encrypted ID + random # sent to 2nd terminal

2nd terminal: Kh Key + random # → KD key (2)

KD key + encrypted ID → IMSI ID (3)

Owada discloses security technique in which a random number is generated and then used as a symmetrical key to encode information. *See* Owada, pgph [0043]. The random number (symmetrical key) is asymmetrically encoded with a public key (asymmetrical key). Id., pgph [0044]. The encoded information and the encoded random number are sent to a processing device. *See* Id., pgph [0045]. At the processing device, the encoded random number is decoded using a private key (2nd asymmetrical key). Id., pgph [0046]. The decoded random number (symmetrical key) is then applied to an algorithm to decode the information. Id.

The process of *Owada* can be summarized as follows:

1st terminal: RAND # (symmetric key) + DATA + Symmetric Algorithm → encoded data (4)

RAND # + 1st Asymmetric Key + Asymmetric Algorithm → encoded symmetric key (5)

2nd terminal: Encoded symmetric key + 2nd asymmetric key + asymmetric algorithm → RAND# (6)

RAND# + Encoded data + Symmetric algorithm → DATA (7)

The Office alleges that these features of *Owada* when combined with *Aura* render Applicant's claims as obvious. Applicant disagrees.

Aura discloses a process in which an ID is encoded at a sending device using a public key. As noted earlier a random number is not used to encode the ID. At a receiving device, random data is used with a private key to compute the public key, which is thereafter used to decode the encoded ID. Specifically, *Aura* discloses that an HLR computes the cipher key Kd (public key) by means of the private key Kh known to it and the random number RAND1 received from a mobile station. *See* Aura, col. 5, lines 33-35.

Owada discloses a process in which the random number is used as the key to encode information. The Office alleges that because *Aura* discloses the use of two keys, it can be readily combined with *Owada* in its use of asymmetrical and symmetrical algorithms. However, the mere fact that one reference discusses the use of public and private keys and another reference discloses the use of asymmetric and symmetric keys does not support the inference that the references are combinable to render the claimed invention as obvious.

For example, as discussed above, *Aura* discloses execution, at a first terminal, of a single function (1) to generate an encrypted ID (encoded data). This single function uses a public key (Kd). A cryptographic hash function is used to generate the key Kd using a Random number and a private key Kh. In comparison, *Owada* discloses the execution of two functions (4) and (5) at a first terminal to generate encoded data and to encode the symmetric key (random #) used to generate the encoded data, respectively. The first function (4) uses a symmetric algorithm with symmetric key (random #) and a second function (5) uses an asymmetric algorithm with asymmetric key. At the second terminal, *Owada* discloses the use of the asymmetric algorithm and a second asymmetric key to

decipher the encoded symmetric key (random #) (6) and then use the symmetric key (random #) in a symmetric algorithm to decipher the encoded data (7).

As should be readily apparent, the *Owada* patent discloses that the Random number or symmetric key is used at a first terminal to encode the information or data. *Owada* also discloses the communication of the cipher key (Random number) over the transmission medium for decoding at a second terminal. In contrast, the *Aura* discloses that the random number is used at a second terminal to calculate the cipher key. One of ordinary skill would understand that the technique used by *Aura* reduces and/or prevents the compromise of the cipher key by not communicating the cipher key Kd over a transmission medium. For at least this reason, one of ordinary skill would not have modified the teachings of *Aura* with those of *Owada* because the latter potentially compromises knowledge of the cipher key (random number) by transmitting the same over a communication medium.

Even when the combination is considered under the flexible motivation test afforded in KSR Int'l v. Teleflex Inc., 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007), there is no evidence that one of ordinary skill possesses the requisite knowledge and skill to modify the references as alleged to achieve the claimed embodiment. Moreover, there is arguable no exemplary rationale provided in *KSR* under which *Aura* and *Owada* can be combined to render the claimed embodiments obvious.

Furthermore, if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959). Namely, because

the features *Owada* change in the basic principle under which *Aura* was designed to operate (i.e., non-transmission of cipher key), the combination cannot be deemed proper to render the claimed embodiments as obvious.

In summary, *Aura* and *Owada* when applied individually or collectively as alleged by the Examiner fail to disclose or suggest every feature and/or the combination of features recited in Applicant's claims. Accordingly, a *prima facie* case of obviousness has not been established.

For rejections under 35 U.S.C. § 103(a) based upon a combination of prior art elements, in KSR Int'l v. Teleflex Inc., 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007), the Supreme Court stated that "a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." "Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some **articulated reasoning with some rational underpinning** to support the legal conclusion of obviousness." In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006) (emphasis added). Applicant believes that the Office has not met this burden. For at least this reason, withdrawal of the rejection under 35 U.S.C. §103 is respectfully requested.

Conclusion

Based on the foregoing amendment and remarks, Applicant respectfully submits that claims 1-11 and 13-16 are allowable and this application is in condition for allowance. Favorable examination and consideration of this application are respectfully requested. In the event any unresolved issues remain, the Examiner is invited to contact Applicant's representative identified below.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: December 17, 2009

By: /Shawn B. Cage/
Shawn B. Cage
Registration No. 51522

Customer No. 21839
703 836 6620